IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | | |
|---|---|---|---|
| First Named Inventor: | Yue Chen | Attorney Docket No.: | 150562.01 |
| Application No.: | 09/758,831 | Group Art Unit | 2182 |
| Filed: | January 11, 2001 | Examiner: | Schneider, J |
| Customer No.: | 22971 | Confirmation Number: | 8533 |
| Title: COMPUTER-BASED SWITCH FOR TESTING NETWORK SERVERS | | | |

## APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Applicant - Microsoft Corporation
**Customer No. 22971**

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits an appeal brief for application 09/758,831, filed January 11, 2001, with a request for a two month extension of time. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

Appeal Brief Items

Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

Status of Claims

Claims 1-31 stand rejected and are pending in the application. Claims 1-31 are appealed. Claims 1-2, 8-9, 17, 24, and 31 were previously amended. No claims have been cancelled. Claims 1-31 are set forth in the Appendix of Appealed Claims.

Status of Amendments

A Final Office Action was issued on March 9, 2007.

Appellant filed a Notice of Appeal on May 9, 2007 in response to the Final Office Action.

No claims have been amended since the issuance of the Final Office Action.

Summary of Claimed Subject Matter

The pending independent claims are claims 1, 9, 17, 24, and 31. A concise explanation of each of the independent claims is provided below.

**Claim 1** is directed to a computer (104, page 12, line 4) functioning as a computer-based network switch (72, page 9, line 25 - page 10, line 4), comprising a first network adapter (102, page 9, line 27) for connecting to an external network (100, page 10, line 18), a plurality of second network adapters (74, 76, 78, page 10, line 13) each for forming a connection with a network server (84, 86, 88, page 10, line 13-14) in a private network (114, page 11, lines 19-24), and a switching component (80, page 10, lines 17-20) for receiving network communication data (90, lines 20-23) from the external network (100, page 10, line 18) through the first network adapter (102, page 9, line 27) and directing the received network communication data (90, lines 20-23) to the second network adapters (74, 76, 78, page 10, line 13) for transmission to the respective network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24).

A test control component (82, page 12, lines 1-2) is for selectively disabling the second network adapters (74, 76, 78, page 10, line 13) to create failure of physical connections (112, page 12, lines 18-19) between the second network adapters (74, 76, 78, page 10, line 13) and the respective network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24).

**Claim 9** is directed to a computer-readable medium (page 6, lines 23-25) having computer-executable components (page 5, lines 1-6) for controlling a

plurality of network adapters (74, 76, 78, page 10, line 13) in a computer (104, page 12, line 4) to create test conditions (page 12, lines 16-27) for testing network servers (84, 86, 88, page 10, line 13-14) in a private network (114, page 11, lines 19-24), the network servers (84, 86, 88, page 10, line 13-14) connected to the network adapters (74, 76, 78, page 10, line 13), comprising a switching component (80, page 10, lines 17-20) for receiving network communication data (90, page 12, lines 20-23) from an external network (100, page 10, line 18) and directing the received network communication data (90, lines 20-23) to the network adapters (74, 76, 78, page 10, line 13) for transmission to the respective network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24).

A test control (82, page 12, lines 1-2) is for selectively disabling the network servers (84, 86, 88, page 10, line 13-14) to create failure of physical connections (page 12, lines 19-21) between the network adapters (74, 76, 78, page 10, line 13) and the respective network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24).

**Claim 17** describes a system (FIG. 2) for testing network servers (84, 86, 88, page 10, line 13-14) in a private network (114, page 11, lines 19-24), comprising a computer (104, page 12, line 4) functioning as a computer-based network switch (72, page 9, line 25 - page 10, line 4), including a plurality of network adapters (74, 76, 78, page 10, line 13) for forming connections to the network servers (84, 86, 88, page 10, line 13-14), a switching component (80, page 10, lines 17-20) for receiving network communication data (90, page 10, lines 20-23) from an external network (100, page 10, line 18) and directing the

received network communication data (90, page 12, lines 20-23) to the network adapters (74, 76, 78, page 10, line 13) for transmission to the respective network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24), and a test control (82, page 12, lines 1-2) for selectively disabling the network adapters (74, 76, 78, page 10, line 13)

A plurality of client computers (92, 94, 96, page 11, lines 7-10) are connected to the external network (100, page 10, line 18) for communication with the network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24) through the computer-based network switch (72, page 9, line 25 - page 10, line 4) and a server testing controller (82, page 12, lines 1-2) connected to the external network (100, page 10, line 18) for coordinating testing of the network servers (84, 86, 88, page 10, line 13-14).

The server testing controller (110, page 12, lines 2-6) instructs the client computers (92, 94, 96, page 11, lines 7-10) to send network communication data (90, page 12, lines 20-23) to the network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24) through the computer-based network switch (72, page 9, line 25 - page 10, line 4), and causes the test control (110, page 12, lines 2-6) to selectively disable the network adapters (74, 76, 78, page 10, line 13) to create failure of physical connections between the network adapters (74, 76, 78, page 10, line 13) and the network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24) connected thereto.

**Claim 24** is directed to a method of testing a plurality of network servers (84, 86, 88, page 10, line 13-14) in a private network (114, page 11, lines 19-24), comprising the steps of connecting the network servers (84, 86, 88, page 10, line 13-14) to a plurality of network adapters(74, 76, 78, page 10, line 13), receiving network communication data (90, page 10, lines 20-23) from an external network (100, page 10, line 18), directing the received network communication data (90, page 10, lines 20-23) to the network adapters (74, 76, 78, page 10, line 13) for transmission to the respective network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24) connected thereto, and selectively disabling the network adapters (74, 76, 78, page 10, line 13) to create failure of physical connections between the network adapters (74, 76, 78, page 10, line 13) and the network servers (84, 86, 88, page 10, line 13-14) in the private network (114, page 11, lines 19-24) connected thereto.

**Claim 31** is directed to a computer (104, page 12, line 4) comprising a first set of network adaptors (74, 76, 78, page 10, line 13) configured to connect the computer (104, page 12, line 4) to a plurality of clients (92, 94, 96, page 11, lines 7-10) through a first network (100, page 10, line 18), a second set of network adaptors (74, 76, 78, page 10, line 13) configured to connect the computer (104, page 12, line 4) to a plurality of servers (84, 86, 88, page 10, line 13-14) through a second network (114, page 11, lines 19-24), a switching module (80, page 10, lines 17-20) configured to identify incoming communication data (90, page 10, lines 20-23) from the clients (92, 94, 96, page 11, lines 7-10) received by the first set of network adaptors (74, 76, 78,

page 10, line 13) and to send the communication data (90, page 10, lines 20-23) to the servers (84, 86, 88, page 10, line 13-14) through the second set of network adaptors (74, 76, 78, page 10, line 13).

A testing module (82, page 12, lines 1-2) is configured to create a failure of a physical connection to at least one of the servers (84, 86, 88, page 10, line 13-14) by disabling the network adaptor corresponding to the at least one server (84, 86, 88, page 10, line 13-14) in the second set of network adaptors (74, 76, 78, page 10, line 13). A fail-over mechanism (page 12, lines 24-27) associated with the plurality of servers (84, 86, 88, page 10, line 13-14) is tested by the failure of the physical connection created by the testing module (82, page 12, lines 1-2).

**Grounds of Rejection to be Reviewed on Appeal**

Claims 1-7, 9-15, 17-22, 24-29, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,314,531 to Kram (hereinafter "Kram") in view of How Networks Work by Derfler (hereinafter "Derfler") and further in view of alleged Applicant Admitted Prior Art.

Claims 1-7, 9-15, 17-22, 24-29, and 31 are also rejected under 35 U.S.C. § 103(a) as being unpatentable over Kram, in view of Derfler, the alleged Applicant Admitted Prior Art, and U.S. Patent 5,862,362 to Somasegar et al. (hereinafter "Somasegar").

Argument

**The rejection to Independent Claims 1, 9, 17, 24, and 31 under 35 U.S.C. §103(a) over the combination of Kram, Derfler, the alleged Applicant Admitted Prior Art, and Somsegar fails to establish a *prima facie* case of obviousness.**

Independent Claims 1, 9, 17, 24, and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kram in view of Derfler and the alleged Applicant Admitted Prior Art. Independent Claims 1, 9, 17, 24, and 31 are also rejected under 35 U.S.C. § 103(a) as being unpatentable over Kram in view of Derfler, the alleged Applicant Admitted Prior Art, and Somasegar. The Applicant respectfully submits that the Office has not established a proper obviousness rejection because Kram in view of Derfler and the alleged Applicant Admitted Prior Art as well as Kram in view of Derfler, the alleged Applicant Admitted Prior Art, and Somasegar fail to establish a *prima facie* case of obviousness.

In particular, either the combination of Kram and Derfler or the combination of Kram and Somasegar fail to teach or suggest all of the limitations of Claims 1, 9, 17, 24, or 31. In addition, there is no motivation to combine either Derfler with Kram or Somasegar with Kram.

SUMMARY OF THE DISCLOSURE IN KRAM, DERFLER, THE ALLEGED APPLICANT ADMITTED PRIOR ART, AND SOMASEGAR

In general, Kram discloses a method and system for emulating network latency and other network performance metrics such that network connected software systems may be tested in a cost effective manner. Kram discloses that

a network emulator that emulates, or duplicates the behavior of, a network. The emulator requires modifications to the media access control (MAC) address and the internet protocol (IP) mapping tables of the computer systems connected to an emulator host computer. Such changes to the MAC-to-IP tables cause network packets to be redirected to an emulator host computer where the packets may be delayed, deleted, corrupted, or otherwise modified to mimic a network disturbance.

Derfler describes basic principles of signaling and information packaging used in all computer systems. Derfler also discloses how such basic principles function within various pieces of network equipment ranging from network interface cards to the Internet. The Office contends the alleged Applicant Admitted Prior Art discloses that private networks are well known in server networks for the Internet.

The Office alleges that the Applicant Admitted Prior Art discloses "private networks are well known in server networks for the Internet" (*see* Final Office Action of 3/9/2007, page 6, point 17). The alleged Applicant Admitted Prior Art is introduced by the Office in the Non-Final Office Action of 06/08/2005. However, the Applicant has never admitted such a disclosure and the Office does not state where such an admission was made.

Somasegar discloses a network failure simulation tool that provides simulation of a network failure suitable for automated software testing under software control. The network failure simulation tool intercepts packets being sent or received by a computer on a network by redirecting the packets from a network input/output architecture to substitute packet handlers.

INDEPENDENT CLAIMS 1, 9, 17, 24, and 31

1. SUBSTANCE OF THE REJECTION

The Final Office Action asserts that Kram discloses all of the subject matter of Claims 1, 9, 17, 24, and 31, but that "Kram fails to explicitly teach the tested element being a switch between an external network and a private network". The Office then asserts that "Derfler teaches that the switching between LANs and WANs was well known in the art" (see Final Office Action of 3/9/2007, page 6, point 17). The Office asserts that the reason to combine the teachings of Derfler with those of Kram is "to provide more robust testing of the fault rich WAN environment". The Office also asserts that the alleged Applicant Admitted Prior Art discloses the same subject matter as Derfler (*see* Final Office Action of 3/9/2007, page 4, point 11).

The Final Office Action also makes a second rejection under 35 U.S.C. 103(a) to Claims 1-7, 9-15, 17-22, 24-29, and 31 as being unpatentable over Kram, Derfler, the alleged Applicant Admitted Prior Art, and Somasegar. The Final Office Action asserts that Kram discloses all of the subject matter of Claims 1, 9, 17, 24, and 31, but that Kram also "does not explicitly call the creation persistent connection failures [of Kram] the 'creation of physical connections'" and continues, "Somasegar teaches that to create failures of physical connections normally caused by unplugging the connection is accomplished by using the substitute handler systems" (*see* Final Office Action of 3/9/2007, page 7, point 18). The Office asserts that one of ordinary skill in

the art would be motivated to combine the teachings of Kram, Derfler, the alleged Applicant Admitted Prior Art, and Somasegar to "test network robustness to better identify errors and verify functionality" (*see* Final Office Action of 3/9/2007, page 7, point 18).

## 2. THE COMBINATION OF KRAM AND DERFLER OR KRAM AND SOMASEGAR DOES NOT TEACH OR SUGGEST ALL CLAIM LIMITATIONS

In a first rejection to Claims 1, 9, 17, 24, and 31 under 35 U.S.C. § 103(a), the Office asserts that Kram discloses "network-switching elements with connections to external networks and connections to network servers" at FIG. 3 and that Kram discloses "emulating such communication persistent failures of physical connections [sic]" at column 3, lines 30-55. The rejection does not draw any specific equivalencies between the subject matter of Kram and the subject matter of Claims 1, 9, 17, 24, or 31, however, the rejection does attempt to draw an equivalency between a failure of a physical connection and an emulated failure.

The Office addresses such an equivalency in the "Response of Arguments" section of the Final Office Action of 3/9/2007, asserting, "Applicant has argued that the emulator [of Kram] does not create failure of physical connections between the second network adapter and the respective network servers in the private network". The Office admits, "[i]t is certainly true that the physical ports [of Kram] do not themselves fail" (emphasis added) before continuing, "but what must be found is that the physical connection fails".

Kram does not discuss "physical ports" and the words "port" or "physical port" do not appear anywhere in the disclosure of Kram. Therefore, it cannot be determined what the Office is referring to when discussing a "physical port". For example, it is known to those skilled in the art that a network adapter functioning in a computer system may include a number of "ports". A "port" may also refer to the physical connection into which a network cable is physically connected.

Regardless, the Office then continues with "[t]he physical failure [of Kram] is not a mechanical failure, but a simulated mechanical failure". An emulated or simulated network failure, such as that disclosed in Kram, is not equivalent to a physical network failure, as is disclosed in Claims 1, 9, 17, 24, and 31. Consider that in the physical failure of a network adapter, the network adapter is no longer physically connected to the network. In contrast, in an emulated or simulated mechanical failure, the network adapter is not only still physically connected to the network but is also still completely functioning. In a test environment Kram could fail to produce realistic collateral failure conditions.

Furthermore, in making out a second rejection under 35 U.S.C. § 103(a), the Office admits that "Kram does not explicitly call the creation persistent connection failures the 'creation of failures of physical connections'" (emphasis added) in contradiction to the first rejection under 35 U.S.C. § 103(a) (*see* Final Office Action of 3/9/2007, page 4, point 11, and page 8, point 18). The Office then asserts that Somasegar discloses the "creation of failures of physical connections" at column 1, line 29 to column 2, line 20.

The cited section of Somasegar does discuss the creation of a network failure *by a human being*, disclosing "[a] brief network failure can be simulated by manually unplugging the network wire connection" and "[t]his test methodology, however, is unsuitable for large scale automated testing" (*see* Somasegar, column 1, lines 29-35). However, Somasegar does not teach the creation of a physical failure in the network being performed by a test component as is disclosed in Claims 1, 9, 17, 24, and 31. Indeed, Somasegar only teaches that a human may unplug a network wire connection to create a physical failure of the wire connection.

2. THERE IS NO MOTIVATION TO COMBINE DERFLER WITH KRAM

The Office asserts that one skilled in the art would be motivated "to combine the network testing of Kram to the external network accesses of private WANs of Derfler and AAPA (Applicant Admitted Prior Art) to provide more robust testing of the fault rich WAN environment" (*see* Final Office Action of 3/9/2007, page 7, point 18). However, neither Kram nor Derfler teaches or suggests "more robust testing", nor does Kram describe a "fault rich WAN environment". There is no evidence of record that suggests a desire or need, prior to the instant invention, for more robust test, nor what that would encompass.

Furthermore, it is not clear from where the Office is quoting the term "fault rich WAN environment" as neither of Kram or Derfler disclose such a term and it is also not clear what is represented by a "fault rich WAN environment".

Therefore, as neither Derfler nor Kram define or describe a "fault rich WAN environment", there can be no motivation to combine the disclosure of Derfler with that of Kram to provide "more robust testing" of such a non-existent "fault rich WAN environment".

2. THERE IS NO MOTIVATION TO COMBINE SOMASEGAR WITH KRAM

The Office asserts that one of ordinary skill in the art would be motivated to combine the "creation of failures of physical connections" of Somasegar with the network test system of Kram "in order to test network robustness to better identify errors and verify functionality" (*see* Final Office Action of 3/9/2007, page 7, point 18). However, as previously discussed, Somasegar does not disclose any creation of a physical failure that may be combined with Kram. In particular, Somasegar only discloses a human being creating a physical failure by unplugging a network wire connection (*see* Somasegar, column 1, lines 29-31). That is, the system and methods of Kram do not offer or suggest any point at which a human may be requested or directed to unplug a network connection.

Furthermore, Kram does not discuss the testing of "network robustness" and it is not clear what the term "network robustness" refers to or why one of ordinary skill in the art would be motivated to test network robustness even if Kram or Somasegar were to disclose such a term. Therefore, one of ordinary skill in the art would not be motivated to combine Somasegar with Kram.

DEPENDENT CLAIMS 2-8, 10-16, 18-23, AND 25-30

Claims 2-8 depend from Independent Claim 1, Claims 10-16 depend from Independent Claim 9, Claims 18-23 depend from Independent Claim 17, and Claims 25-30 depend from Independent Claim 24, and are patentable at least by virtue of such dependency.

Conclusion

The Office's basis and supporting rationale for the § 103(a) rejections is not supported by the disclosure of the cited references. Applicant respectfully requests that the rejections be overturned and that the pending claims be allowed to issue.

Respectfully Submitted,

Dated: August 9, 2007 By: /James T. Strom/

James T. Strom
Reg. No. 48,702
Microsoft Corporation
One Microsoft Way,
Redmond, WA 98052
Drafted by Peter Taylor

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence and the documents identified on this form are being electronically deposited with the USPTO via EFS-Web on the date shown below:

August 9, 2007 /Kate Marochkina/

Date Kate Marochkina

Appendix of Appealed Claims

1. A computer functioning as a computer-based network switch, comprising:

a first network adapter for connecting to an external network;

a plurality of second network adapters each for forming a connection with a network server in a private network;

a switching component for receiving network communication data from the external network through the first network adapter and directing the received network communication data to the second network adapters for transmission to the respective network servers in the private network connected thereto; and

a test control component for selectively disabling the second network adapters to create failure of physical connections between the second network adapters and the respective network servers in the private network connected thereto.

2. A computer as in claim 1, further including a third network adapter for connecting the test control component to the external network to allow the test control component to communicate with the external network.

3. A computer as in claim 1, wherein the switching component is programmed to operate on network communication data passing therethrough to create a communication test condition other than a connection failure condition.

4. A computer as in claim 3, wherein the switching component is programmed to delay network communication data passing therethrough.

5. A computer as in claim 3, wherein the switching component is programmed to selectively drop network communication data.

6. A computer as in claim 3, wherein the switching component is programmed to reorder data in a communication stream passing therethrough.

7. A computer as in claim 3, wherein the switching component is programmed to introduce errors into network communication data passing therethrough.

8. A computer as in claim 1, wherein the switching component is programmed for monitoring flows of network communication data therethrough from the respective network servers in the private network to the external network.

9. A computer-readable medium having computer-executable components for controlling a plurality of network adapters in a computer to create test conditions for testing network servers in a private network, the network servers connected to the network adapters, comprising:

a switching component for receiving network communication data from an external network and directing the received network communication data to the network adapters for transmission to the respective network servers in the private network connected thereto;



Microsoft Corporation
Application No. 09/758,831
Docket No.150562.01
Filing Date: Jan 11, 2001

a test control for selectively disabling the network servers to create failure of physical connections between the network adapters and the respective network servers in the private network connected thereto.

10. A computer-readable medium as in claim 9, wherein the switching component includes further computer-executable instructions for operating on network communication data passing therethrough to create a test condition other than a connection failure condition.

11. A computer-readable medium as in claim 10, wherein the switching component includes computer-executable instructions for selectively buffering network communication data passing therethrough for a delay period.

12. A computer-readable medium as in claim 10, wherein the switching component includes computer-executable instructions for selectively dropping network communication data passing therethrough.

13. A computer-readable medium as in claim 10, wherein the switching component includes computer-executable instructions for reordering data in a communication stream passing therethrough.

14. A computer-readable medium as in claim 10, wherein the switching component includes computer-executable instructions for introducing errors into network communication data passing therethrough.

15. A computer-readable medium as in claim 9, wherein the test control includes computer-executable instructions for communicating with a server testing controller to receive commands regarding testing of the network servers.

16. A computer-readable medium as in claim 9, wherein the switching component includes further computer-executable instructions for monitoring flows of network communication data from the respective network servers to the external network.

17. A system for testing network servers in a private network, comprising:

a computer functioning as a computer-based network switch, including a plurality of network adapters for forming connections to the network servers, a switching component for receiving network communication data from an external network and directing the received network communication data to the network adapters for transmission to the respective network servers in the private network connected thereto, and a test control for selectively disabling the network adapters;

a plurality of client computers connected to the external network for communication with the network servers in the private network through the computer-based network switch;

a server testing controller connected to the external network for coordinating testing of the network servers, including instructing the client computers to send network communication data to the network servers in the private network through the computer-based network switch, and causing the test control to selectively disable the network adapters to create failure of

physical connections between the network adapters and the network servers in the private network connected thereto.

18. A system as in claim 17, wherein the switching component is controllable to operate on network communication data passing therethrough to create a test condition other than a connection failure condition.

19. A system as in claim 18, wherein the switching component is controllable to selectively buffer network communication data passing therethrough to introduce a delay.

20. A system as in claim 18, wherein the switching component is controllable to selectively drop network communication data passing therethrough.

21. A system as in claim 18, wherein the switching component is controllable to reorder network communication data passing therethrough.

22. A system as in claim 18, wherein the switching component is controllable to introduce errors in network communication data passing therethrough.

23. A system as in claim 17, wherein the switching component is programmed for monitoring flows of network communication data from the network servers to the network clients.

24. A method of testing a plurality of network servers in a private network, comprising the steps of:

connecting the network servers to a plurality of network adapters;

receiving network communication data from an external network;

directing the received network communication data to the network adapters for transmission to the respective network servers in the private network connected thereto;

selectively disabling the network adapters to create failure of physical connections between the network adapters and the network servers in the private network connected thereto.

25. A method as in claim 24, further including the step of operating on the network communication data received from the external network to create a test condition other than a connection failure condition before sending the network communication data to the network servers through the network adapters.

26. A method as in claim 25, wherein the step of operating includes selectively buffering network communication data passing therethrough for a delay period.

27. A method as in claim 25, wherein the step of operating includes selectively dropping network communication data passing therethrough.

28. A method as in claim 25, wherein the step of operating includes reordering network communication data passing therethrough.



Microsoft Corporation
Application No. 09/758,831
Docket No.150562.01
Filing Date: Jan 11, 2001

29. A method as in claim 25, wherein the step of operating includes introducing errors to network communication data passing therethrough.

30. A method as in claim 24, further including the step of monitoring flows of network communication data from the network servers to the external network..

31. A computer comprising:

a first set of network adaptors configured to connect the computer to a plurality of clients through a first network;

a second set of network adaptors configured to connect the computer to a plurality of servers through a second network;

a switching module configured to identify incoming communication data from the clients received by the first set of network adaptors and to send the communication data to the servers through the second set of network adaptors; and

a testing module configured to create a failure of a physical connection to at least one of the servers by disabling the network adaptor corresponding to the at least one server in the second set of network adaptors;

wherein a fail-over mechanism associated with the plurality of servers is tested by the failure of the physical connection created by the testing module.

Evidence Appendix

None

Related Proceedings Appendix

None